IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 19-369
	)	
LAFON ELLIS	)	

REPLY TO GOVERNMENT'S PRETRIAL MOTIONS

This pleading is intended to reply to the following pleadings filed by the United States: Motion to Quash Subpoena (ECF No. 47) and Omnibus Response to Defendant's Pretrial Motions (ECF No. 108).

INTRODUCTION

The government wants to introduce information from a statistical report generated by TrueAllele software that purports to link Mr. Ellis to a gun. TrueAllele purports to generate statistical values associated with DNA match evidence using data from samples deemed inconclusive by other interpretation methods, and those statistical values are used to infer whether or not Mr. Ellis's DNA may be present. The software took data that was deemed inconclusive by traditional DNA interpretation methods, and produced strongly inculpatory match statistics for the very same evidence. To inspect the reliability of this statistical evidence, "the match," Mr. Ellis sought production of verification and validation ("V&V") materials, including but not limited to the source code of TrueAllele. The sought-after material exists, and is specifically tailored using precise terms of art based on industry standards for evaluation and verification and validation of PG software systems like TrueAllele. Prior to applying for the subpoena for these materials, the Defense first asked the government for them. After being denied access, the Defense filed their subpoena to Cybergenetics.

As with other PG programs, TrueAllele results cannot be objectively verified. The only real means to determine whether the statistics are properly, or accurately, calculated and that the assumptions used by the software program have been properly validated is through inspection of the program's source code. The government wants to require Mr. Ellis, and this Court, to accept the government's technical or scientific conclusions because a developer with a financial interest in, and who holds a patent for, the software makes a trade secret claim, and testifies around the country that his program is flawless and does not require independent review and inspection.

The lack of independent review raises serious concerns about the reliability of the validation studies cited by the government and was the chief criticism of PG software, including TrueAllele, in a 2016 report by the President's Council of Advisors on Science and Technology (the "PCAST Report"). *See* President's Council of Advisors on Sci. & Tech., Exec. Office of the President, *Forensic Science in Criminal Courts: Ensuring Scientific Validity of Feature-Comparison Method* 78–81 (Sept. 2016), https://bit.ly/34D6L1X. "The President's Council of Advisors on Science and Technology (PCAST) is an advisory group of the **Nation's leading scientists and engineers**, appointed by the President to augment the science and technology advice available to him from inside the White House and from cabinet departments and other Federal agencies." *Id*. at 4 (emphasis added). One of the goals of PCAST was to "help ensure the validity of forensic evidence used in the Nation's legal system." *Id*. at x. PCAST cautioned that while PG programs, specifically mentioning TrueAllele and STRmix, "clearly represent a major improvement over purely subjective interpretation," they still require careful scrutiny to determine "whether the methods are scientifically valid" and "whether the software correctly implements the methods." *Id*. at 8. In their report, PCAST writes that they "consulted with John Butler, Special Assistant to the Director for Forensic Science at NIST and Vice Chair of the NCFS. Butler

concurred with PCAST's finding." *Id*. at 81. Dr. Butler "is a world authority on forensic DNA analysis, whose Ph.D. research, conducted at the FBI Laboratory, pioneered techniques of modern forensic DNA analysis and who has written five widely acclaimed textbooks on forensic DNA typing." *Id*. at 81 n.220. Dr. Perlin, the owner of Cybergenetics and creator of TrueAllele, disagrees with the nation's leading scientist and engineers who represent the PCAST group, as well as Dr. Butler, the world authority on forensic DNA analysis. *See*, Letter Rebuking Dr. John Holdren, PCAST co-chair, published on Cybergenetics website.[1]

Preventing the Defense, and their experts, from accessing, reviewing, or inspecting the sought-after materials would not only violate Mr. Ellis's rights to compulsory process, but also blunt the truth-seeking quality of the adversarial process by preventing the Defense from meaningfully challenging the government's expert. This in turn would prevent the Court from receiving all relevant information about the reliability of the government's scientific expert and testimony. Such crucial lack of information, would prevent this Court from fulfilling her "gatekeeping" role pursuant *Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 589 (1993).

The government confidently writes that TrueAllele has been "found to be reliable by every court to consider its admissibility." *See* ECF No. 108 at 4. This is absolutely false. By way of independent investigation, the Defense found out that the Honorable Justice Jamie Campbell excluded TrueAllele in a late 2019 Canadian murder prosecution. *See R. v. Dechamp*, 2019 NSSC 367 (N.S. Dec. 10, 2019) (excluding TrueAllele after an admissibility hearing with three and a half days of testimony from Dr. Perlin at which he provided the court with 15 volumes of materials), Opinion Excluding TrueAllele, attached as Exhibit 1. Although arguments for V&V materials, including source code, were made by the defense in *Dechamp*, Judge Campbell wrote in her

[1] Available at, https://www.cybgen.com/information/newsroom/2016/sep/files/letter.pdf.

opinion that she did not need to rule on that matter because she did not find TrueAllele to be admissible either way. One can only wonder why the government, or their expert, failed to mention this case to the Defense, or the Court as part of their list of cases where TrueAllele has been admitted.[2]

Additionally, a United States District Judge recently excluded PG software STRmix™ after granting defense counsel access to review and inspect the V&V materials, including source code of STRmix™, over the government's objection. *See United States v. Gissantaner*, 417 F. Supp. 3d 857, 864 (W.D. Mich. 2019) (Neff, J.) (excluding PG software STRmix™ in a three-person complex mixture case after granting defense review of source code).[3] STRmix™ is TrueAllele's main competitor,[4] and unlike TrueAllele, STRmix™ has been approved and routinely used by the FBI Laboratory since 2014.[5] Nathan Adams, was hired by the defense team in *Gissantaner*. He reviewed the source code and wrote a report to the Judge that was used at the *Daubert* hearing. *Gissantaner*, 417 F. Supp. 3d 857 at 868. Mr. Adams was also hired by the Defense in this case, and at the request of the Defense wrote a declaration in this case explaining the necessity to inspect the V&V materials, including source code. *See* Decl. Nathan Adams, attached as Exhibit 2. The court in *Gissantaner* "appointed two experts, Dr. Michael Coble and Dr. Dan E. Krane, both well-recognized for their specialized expertise and contributions to the advancing field of probabilistic genotyping in forensic DNA analysis in the U.S." *See Gissantaner*, 417 F. Supp. 3d 857 at 860. Dr. Krane was hired by the Defense in this case and at the request of

[2] The government did mention a recent Virginia decision where the court issued an Order compelling Cybergenetics to produce its source code. *See* ECF. No. 108 at 6 n.2

[3] Mr. Ellis would like to remind the Court that TrueAllele reported the results in Mr. Ellis's case in a 4-person complex mixture.

[4] TrueAllele filed a patent infringement suit against the company that owns STRmix™. *See Cybergenetics v. Inst. of Envtl. Sci. & Research*, No. 5:19-cv-1197-SL (N.D. Ohio).

[5] The Defense is in no way conceding that the use of the software by the FBI means it is reliable, but it does give STRmix™ an edge over TrueAllele which has not been adopted by the FBI.

the Defense wrote a declaration in this case arguing for the necessity to inspect the V&V materials, including source code. *See* Decl. Dan E. Krane, PhD, attached as Exhibit 3.

Another United States District Judge, in *United States v. Kevin Johnson*, No. 15-cr-565 (S.D.N.Y.), presided over a case where the government intended to use competitor PG software Forensic Statistical Tool ("FST"). Over the objection of the government and the developers of FST software, the Honorable Judge Valerie E. Caproni granted the Defense team's Rule 17(c) subpoena for FST's V&V materials, including source code. *See United States v. Kevin Johnson,* No. 15-565, ECF No. 57 (S.D.N.Y. June 7, 2016) (Caproni, J.) (granting defendant's Rule 17(c) subpoena for FST source code); *see also* Lauren Kirchner, *Traces of Crime: How New York's DNA Techniques Became Tainted*, N.Y. Times (Sept. 4, 2017).[6] The review of FST source code in *Johnson* revealed that the software employed in casework functions in ways not reflected in, and even counter to, the methodology that was validated by its developer and described in publications—the very publications relied on by the lab in arguing the reliability of the results generated by the program. Kirchner, *supra*. The differences between how the program actually functions and how the publications said it functions affected countless criminal cases. Because *Johnson* was the first time FST's proprietary code was reviewed, its hidden function had escaped detection in use and in peer review. It was only uncovered because a defense expert was able to review the code pursuant to the court-ordered subpoena. Despite disclosure of the source code, the case never made it to a *Daubert* hearing because the government wrote a letter that it no longer intended to offer the DNA evidence at trial. *See Johnson,* No. 15-565, ECF. No. 119. Despite not being excluded in Federal court, FST has been excluded in State court. *See People v. Collins*, 15 N.Y.S.3d 564 (N.Y. Sup. Ct. 2015) (Excluding probabilistic genotyping software forensic statistical tool as not generally

[6] Available at https://www.nytimes.com/2017/09/04/nyregion/dna-analysis-evidence-new-york-disputed-techniques html.

accepted as reliable in the forensic scientific community under the *Frye* standard in a three-person complex mixture case). Once these flaws were discovered, a high-profile conviction based on FST analysis was overturned. *See* Alan Feuer, *Hasidic Man Convicted of Beating Black Student Gets Verdict Overturned*, N.Y. Times (Oct. 10, 2018).

As Mr. Ellis has articulated repeatedly, the information sought in the subpoena is necessary, and material, to the preparation of his defense. Under the Federal Rules of Criminal Procedure and the Constitution, Mr. Ellis is entitled to gather evidence to be used in his defense. If the information is in the possession, custody, or control of the government, Rule 16 is the appropriate vehicle for obtaining the requested material. If it is not, a valid Rule 17(c) subpoena is. The government has now conceded that it does not have access to the requested information, *see* ECF No. 108 at 8, and as discussed more below, the subpoena is valid. Thus, Mr. Ellis respectfully requests the Court to deny the motion to quash, enter a protective order, and compel Cybergenetics to produce the requested materials. In support of these arguments, Mr. Ellis avers:

I. THE GOVERNMENT LACKS STANDING TO QUASH THE SUBPOENA SERVED TO THIRD-PARTY SOFTWARE COMPANY CYBERGENETICS AND EVEN IF THIS COURT FINDS THAT THE GOVERNMENT DOES HAVE STANDING, THE GOVERNMENT HAS FAILED TO MEET THEIR "HEAVY BURDEN" TO DEMONSTRATE WHY THE SUBPOENA, WITH THE DEFENSE'S PROPOSED MODIFICATIONS, SHOULD BE QUASHED FOR BEING "UNREASONABLE OR OPPRESSIVE."

A. The Government Lacks Standing.

"The government may challenge a subpoena *duces tecum* issued to a third party if the government has a legitimate interest related to the materials sought." *United States. v. Ocasio*, EP-11-cr-2728-KC, 2013 WL 12442496, at *2 (W.D. Tex. May 28, 2013) (granting defense motion to compel and **denying government's motion to quash** a request for subpoenas **seeking the source code from a third-party software company** when defendant challenged the government's

use of "child protection system" software in a Fourth Amendment suppression motion). "In many instances, the opposing party in a criminal case will lack standing to challenge a subpoena issued to a third party because of the absence of a claim of privilege, or the absence of a proprietary interest in the subpoenaed material or of some other interest in the subpoenaed documents." *United States v. Beckford*, 964 F. Supp. 1010, 1023 (E.D. Va. 1997); *United States v. Nachamie*, 91 F. Supp. 2d 552, 558 (S.D.N.Y. 2000) (same); *Ponsford v. United States*, 771 F.2d 1305, 1308 (9th Cir. 1985) (absent proprietary interest in documents sought, no standing to quash); *United States v. Tomison*, 969 F. Supp. 587, 589–95 (E.D. Cal. 1997) (standing only when "legitimate interest" while rejecting government's standing claim that the government is "in the best position to assist the court in ensuring that Rule 17(c) is not being improperly used as a discovery device" and explaining that "the contention does not demonstrate that the government has any of the interests required for a party to have standing to quash a subpoena").

The government has elected to champion the cause of Cybergenetics, but lacks standing because the government does not have a propriety interest, claim of privilege, or personal right in the materials subpoenaed from Cybergenetics. Here, the government argues it has standing to challenge a third-party subpoena based on several arguments: [1] the defense has asked the government to bear costs of the subpoena, therefore the government has standing, *see* ECF. No. 108 at 23; [2] the government "has a legitimate interest in preventing [the defendant] from using a subpoena to obtain discovery materials that would otherwise be protected from disclosure," *see* ECF. No. 108 at 24 (citing to *United States v. Vasquez*, 258 F.R.D. 68, 71–72 (E.D.N.Y. 2009) (citing *United States v. Louis*, 2005 WL 180885, at *5 (S.D.N.Y. Jan. 27, 2005))); [3] the government has standing to prevent "undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [a witness's] credibility," *see* ECF. No.108 at 24, (citing

to *United States v. Raineri*, 670 F.2d 702, 712 (7th Cir. 1982); *United States v. Orena*, 883 F. Supp. 849, 869 (E.D.N.Y. 1995)); [4] the government has standing based on 18 U.S.C. § 1835(a), which provides that the United States may take an interlocutory appeal of any decision or order of a district court "authorizing or directing the disclosure of any trade secret." Here, the government's arguments, based on the facts of this case, are unavailing, and the cases they cite are distinguishable. Each argument will be discussed in term:

[1] The defense has asked the government to bear costs of the subpoena, therefore the government has standing, *see* ECF. No. 108 at 23.

The government writes that "it is difficult to imagine how the defendant can both request that the costs be borne by the government and simultaneously claim that the government lacks standing to object to the subpoena." *See* ECF. No. 108 at 23. The government does not cite any opinions in favor of conferring standing based on an indigent defendant's request for the government to bear costs of the subpoena. Notably, the government fails to rebut any of the authority cited by the Defense in their response brief on the topic of who bears the costs, *see* ECF No. 71 at 32 (citing, *United States. v. Florack*, 838 F. Supp. 77, 79 (W.D.N.Y. 1993); *Johnson v. Lamas*, No. 10-cv5326, 2011 WL 2982692, at *3 (E.D. Pa. July 21, 2011); Wright & Miller, 2 Fed. Prac. & Proc. Crim. § 273). This Court should reject the government's novel argument to adopt a bright-line rule that confers the government automatic standing to challenge a third-party subpoena served by an indigent defendant.

[2] The government "has a legitimate interest in preventing [the defendant] from using a subpoena to obtain discovery materials that would otherwise be protected from disclosure," *see* ECF. No. 108 at 24.

In their second attempt to establish standing, the government cites to *Vasquez*, 258 F.R.D. at 71–72, and *Louis*, 2005 WL 180885, at *5, for the proposition that courts have found that the prosecution has standing to move to quash a defendant's third-party subpoena in a criminal case

where it has a legitimate interest in preventing the defendant from using a subpoena to obtain discovery materials that would otherwise be protected from disclosure. While the Defense concedes that courts have found standing under such theory, the facts of the case at bar differ significantly from the cases and reasoning of the cases cited by the government. In *Vasquez*, the defendant—who was charged with racketeering, among other things—served a subpoena on the Nassau County Police Department seeking any and all records, including witness statements, that pertained to the homicides of individuals pursuant to the charged racketeering enterprise. *Id*. at 71. Nassau County moved to quash under Rule 17(h) for subpoenaing witness statements, and claimed law enforcement privilege for other materials. *Id*. The government later moved to quash as well. *Id*. The defendant moved to quash arguing the government lacks standing to quash a subpoena served on a third-party. *Id*. Prior to ruling, the court stated, "[o]ne important question that Courts have considered in deciding the issue of standing is "whether the subpoenaed party joins in the Government's motion to quash." *Id*. at 71. The *Vasquez* court held the government had standing "because, at least in part, Nassau has joined in their application and the Government has a legitimate interest in preventing Castro from using a subpoena to obtain discovery materials that would otherwise be protected from disclosure." *Id*. at 71-71 (citing *Louis*, 2005 WL 180885, at *5 (finding that the Government had standing to quash a subpoena served on the Port Authority where, among other things, the federal prosecution arose out of a Port Authority investigation and the Port Authority joined the Government in seeking to quash the subpoena)).

Vasquez and *Louis* are distinguishable and not on point. First, both cases cite the need for the subpoenaed party to join the government in litigation by filing their own motion to quash. Here, despite being served in early May 2020—six months ago—Cybergenetics has failed to file their own motion to quash a subpoena directed at them. Rule 17(c)(2) states with specificity, "**[o]n**

motion made promptly, the court may quash or modify the subpoena if compliance would be unreasonable or oppressive." (Emphasis added). Using the government's own words, "it is difficult to imagine" how Cybergenetics is going to argue that a motion to quash filed by them six months after it was served to them is made "promptly" as required by Rule 17(c)(2).

Second, *Vasquez* deals with the government attempting to quash a subpoena served to law enforcement (Nassau County Police Department) for items that are in clear violation of Rule 17(h) (witness statements), *i.e.*, materials that would otherwise be protected from disclosure based on Rule 17 itself. Likewise, the government in *Louis* moved to quash a subpoena directed at the Port Authority of New York/New Jersey for allegations of a crime that happened at LaGuardia Airport. *Louis*, 2005 WL 180885, at *1. In holding that the government had standing, the *Louis* court highlighted the fact that the "instant federal prosecution grew out of a PANY/NJ investigation." *Id*. Unlike *Vasquez* and *Louis*, here, the third-party subpoena is neither directed at law enforcement (*Vasquez*) nor quasi law-enforcement (*Louis*). Instead, the subpoena is directed to a third-party for-profit software company. Moreover, unlike *Louis*, the federal prosecution here did not grow out of an incident at the place being subpoenaed.

Instead of relying on the government's cases, the Defense urges this Court to follow *United States, v. Ocasio*, EP-11-CR-2728-KC, 2013 WL 12442496, at *1 (W.D. Tex. May 28, 2013) as a case both helpful and analogous to the issues of first impression regarding a federal subpoena to request software verification and validation materials, including source code, from a third-party software developer. In *Ocasio*, the court granted the defense's motion to compel the source code from a third-party software company while simultaneously holding that the government lacked standing to challenge the subpoena. *Id*. at *4. A detailed summary of that case is outlined in the Defense's Response to Government's Motion to Quash. *See* ECF No. 71 at 12.

[3] <u>The government has standing to prevent "undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [a witness's] credibility," *see* ECF. No. 108 at 24</u>.

For their third argument, the government cites to *Raineri*, 670 F.2d at 712, and *Orena*, 883 F. Supp. at 869, for standing under the theory of preventing "undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [a witness's] credibility." It is worth noting that the *Ocasio* Court cited these cases, *id*. at *2, yet still held that the government lacked standing to challenge a subpoena directed at a third-party software developer. *Id*. at *4.

The factual circumstances in the cases cited by the government, *Raineri* and *Orena*, are in no way comparable to those presented here. In *Raineri*, the Seventh Circuit affirmed the trial court's decision to grant a prosecutor's motion to quash a defendant's subpoena to recall a witness during a criminal trial. In that case, an out-of-state witness traveled to testify for the prosecution and a month later, the defense subpoenaed that same witness to reappear as a defense witness. 670 F.2d at 712. During the government's case in chief, the defendant had an opportunity to cross-examine the witness and launched an "extensive attack" on the witness's credibility. *Id.* The defendant in *Raineri* asserted on appeal that the prosecutor lacked standing to challenge defendant's subpoena to recall the witness. The Seventh Circuit found no error, stating that:

> [T]he prosecution's standing rested upon its interest in preventing undue lengthening of the trial, undue harassment of its witness, and prejudicial over-emphasis on [the witness's] credibility. . . . When, as here, the defendant has already subjected the witness to an intense and complete cross-examination, a trial judge's refusal to recall the witness for further cross-examination does not violate the defendant's right to confront the witness against him."

Id.

In the second case relied on by the Government, *United States v. Orena,* defense counsel subpoenaed records from the accountant of a government witness. 883 F. Supp. 849 at 869. The case involved the prosecution of defendants allegedly aligned with a faction of an organized crime family for conspiring to murder members of a rival faction and for using and carrying firearms

during and in relation to crimes of violence. *Id.* at 853. The defendants were seeking detailed information about a witness's financial transactions. *Id.* at 869. The Government moved to quash the subpoena and the defendant challenged the Government's standing to do so. *Id.* The *Orena* court held that because the subpoena might unduly lengthen the trial and unduly harass the witness and his family, the Government had standing. Unlike this matter, however, *Orena* involved a request for information irrelevant to the current prosecution and involved real potential for danger to its witnesses.

The government has not asserted a legitimate interest in quashing this subpoena. In both *Raineri* and *Orena*, the government sought to quash a subpoena that they argued would cause undue harassment to an individual fact witness. These cases can be distinguished from the case at hand because the witness at issue is not an individual, but instead is a local company that produces a product which the prosecution would like to use in their case-in-chief. This is a company that is in the business of state and federal criminal litigation. Cybergenetics is paid for their time and participation in this matter; therefore, being subject to a third-party subpoena is not harassment. It is simply part of litigation.

[4] The government has standing based on 18 U.S.C. § 1835(a), which provides that the United States may take an interlocutory appeal of any decision or order of a district court "authorizing or directing the disclosure of any trade secret."

The government lastly argues that it has standing based on an interest in protecting Cybergenetics' trade secrets citing to H.R. Rep. No. 104-788, at 13 (1996), reprinted in 1996 U.S.C.C.A.N. 4021, 4032 (discussing 18 U.S.C. § 1835, which authorizes courts to preserve the confidentiality of alleged trade secrets in economic espionage prosecutions because "[w]ithout such a provision, owners may be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth"; and 18

U.S.C. § 1835(a), which provides that the United States may take an interlocutory appeal of any decision or order of a district court "authorizing or directing the disclosure of any trade secret." *See* ECF No. 108 at 24. The arguments are unavailing and their citations are misplaced. First, the congressional report cited is about the passage of the Economic Espionage Act of 1996, which criminalizes economic espionage and theft of trade secrets. The language cited is specifically about prosecutions for the activities criminalized **by that act**. Not all prosecutions. *See* H.R. REP. 104-788, at *4 ("The bill requires courts hearing cases brought under the statute to enter such orders as may be necessary to protect the confidentiality of **the information involved in the case**." (emphasis addded)). Second, the government quotes 18 U.S.C. § 1835(a), but leaves out some key language. The provision states: "In any prosecution or other proceeding **under this chapter**, the court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws . . . ." The chapter is Chapter 90, "Protection of Trade Secrets," and covers the crimes of economic espionage and theft of trade secrets—neither of which is relevant to Mr. Ellis's case. The same is true for the government's citation to 18 U.S.C. § 1835(b). *See* ECF No. 108 at 25 (stating that "the Court also must ensure compliance with 18 U.S.C. § 1835(b), which gives trade-secret owners the right to be heard before a court authorizes or directs the disclosure of any information asserted to be a trade secret.") 18 U.S.C. § 1835(b), like § 1835(a), only covers disclosure of confidential information during a prosecution for economic espionage and theft of trade secrets. Here, Mr. Ellis is charged with neither. Therefore, based on congressional intent and a reading of the entire statute, and not just a portion, these provisions do not apply in this case.

Thirdly, the government has been advancing Cybergenetics' interests so far (*e.g.*, in the motion to quash). Rather than moving to quash the subpoena it was properly served with, Cybergenetics brought it to the government so the government could litigate a motion to quash on its behalf. During the six months that have passed since Cybergenetics has been served, they have failed to raise their hand and object to the subpoena themselves. The company has had a chance to show up, and it has failed to do so.

B. <u>The government has failed to meet their "heavy burden" to demonstrate why the subpoena should be quashed for being "unreasonable or oppressive."</u>

The party seeking to quash the subpoena carries a "heavy burden of proof." *See In re Actiq Sales and Mktg. Practices Litig.*, 07-cv-4492-PBT, 2011 WL 5509434, at *2 (W.D. Pa. Nov. 10, 2011) (Conti, J.) ("A party seeking to quash a subpoena bears a heavy burden of proof."); *In re Grand Jury Proceedings*, 914 F.2d 1372, 1374 (9th Cir. 1990) (same); *In re Grand Jury Investigation*, 610 F.2d 202, 219 (5th Cir. 1980) (same).

There are only two legal grounds to quash a subpoena *duces tecum*: [1] the subpoena "unreasonable," and/or [2] the subpoena "oppressive." *See United States v. Nixon*, 418 U.S. 683, 698 (1974) ("A subpoena for documents may be quashed if their production would be **'unreasonable or oppressive,' but not otherwise**." (emphasis added)).

Mr. Ellis dedicated over fourteen pages of argument in support of why his subpoena is in compliance with Rule 17(c), and the four-factor test in *Nixon*. Each factor was specifically addressed; case law was provided and analogized. *See* ECF No. 71 at 19–32. In blatant contrast, the government not only failed to respond to Mr. Ellis's arguments concerning compliance with the *Nixon* test, but notably failed to argue how Mr. Ellis's subpoena is "unreasonable" or "oppressive" under the *Nixon* standard. The government's briefs speak for themselves; the vast majority of their arguments were addressed by the modifications made by the Defense. What's left

of their arguments for unreasonableness or oppressiveness are conclusory allegations of the validity of their black box algorithm. The government cites to other courts that admitted TrueAllele, but those courts either use a different standard (*Frye*), were not provided with all the necessary information from the defense, or blindly relied on TrueAllele's reliability based on the fact that it has been peer-reviewed, yet ignored the fact that the peer-reviewed studies have Dr. Perlin as a co-author, and that the studies don't actually review the software, *i.e.*, no V&V materials are source code is reviewed as part of those studies. *See e.g.*, *Commonwealth v. Foley*, 38 A.3d 882, 889–90 (Pa. Super. 2012) (citing peer-reviewed studies as a reason why TrueAllele is reliable and then citing to the following two studies where Dr. Perlin is a co-author as proof). The Pennsylvania Superior Court reasoned that because "[b]oth of these papers were published in peer-reviewed journals; thus, their contents were reviewed by other scholars in the field." And "[b]ecause Foley has failed to establish the existence of a legitimate dispute over Dr. Perlin's methodology, he has failed to show that Dr. Perlin's testimony constituted 'novel' scientific evidence. Therefore, we find that the trial court's decision to admit the testimony was not an abuse of discretion. Absent a legitimate dispute, there is no reason to 'impede admissibility of evidence that will aid the trier of fact in the search for truth.'" *Id*. at 890. Based on the Pennsylvania Superior Court's decision in *Foley*, an avalanche of decisions have followed admitting TrueAllele.

In order to counter the government's narrative that peer-review and validation studies mean that TrueAllele is reliable, the Defense hired Dr. Heimdahl and Dr. Matthews, who are experts in engineering, testing, and validating computer systems, including forensic software. Dr. Heimdahl and Dr. Matthews wrote a declaration at the request of the Defense in order to aid this Court's understanding of the need for the V&V materials, including source code. *See*, Decl. of Dr.

Heimdahl and Dr. Matthews attached as Exhibit 4. On the subject of validation studies, Dr. Heimdahl and Dr. Matthews write:

> The prosecution in this case writes that TrueAllele has been subject to "Over thirty-five validation studies . . . to establish the reliability of the TrueAllele method and software. Eight of these studies have been published in peer-reviewed scientific journals, for both laboratory-generated and casework DNA samples." See Doc. No. 108 at 5.
>
> We examined each of the validation studies provided by the prosecution in preparation for this declaration (a total of 39 documents including 9 documents classified as peer reviewed articles). We focused on the 9 peer reviewed articles and concluded the following: 1) The validation studies were not independent, 2) The validation studies did nothing to address the quality of the implementation or likelihood of implementation errors and 3) The validation studies were incomplete. We also point out that peer review of validation studies is simply not the same as software validation and verification. Peer review in a scientific journal indicates only that the reviewers thought the scientific community should see the results, not that the software is reliable enough to be used in the criminal justice system in general or in any specific case in particular.

Exhibit 4 at ¶ 41-42. Dr. Heimdahl and Dr. Matthews go into detail about each of the three flawed areas of the "validation studies." According to their review,

> Perlin himself is an author of 7 of the 9 documents classified as peer reviewed articles and in another the authors explicitly acknowledged the "helpful comments and guidance provided by Dr. Mark Perlin, Matthew Legler, and William Allan of Cybergenetics." The last peer reviewed paper explicitly states that "This paper does not address the application of the TrueAllele expert review system to the analysis of forensic samples." Exhibit 4 at ¶ 43.
>
> None of the validation studies cited by the prosecution in this case are addressing the problem of assessing the overall correctness of the implementation of the TrueAllele sourcecode. Dr Perlin's own declaration states "Source code is not used in validation studies." . . . Without access to the program source code as well as all supporting software development artifacts, researchers can say no more than that the results generated by the program are plausible for the few test cases that were executed. But, the software could appear to produce plausible results while still concealing latent errors. *See* Exhibit 4 at ¶ 45-46.
>
> Peer review in a scientific journal only indicates that the reviewers thought the scientific community should see the results, not that the software is reliable enough to be used in the criminal justice system in general or in any specific case in particular. *Id*. at 51.

For all the reasons listed in Mr. Ellis's brief regarding compliance with the four-factor *Nixon* test, *see* ECF No. 71 at 19–32, and because the government's response briefs are notable for what they fail to address: why the subpoena should be quashed as unreasonable and or oppressive, this Court should grant the subpoena to Cybergenetics consistent with the proposed modifications in ¶ 23 of Mr. Ellis's Response Brief.

C. Trade secrets are not an appropriate reason to quash the subpoena, and the use of court-issued protective orders are commonly used when trade secrets are disclosed to opposing counsel and their experts for review.

The government, on behalf of Cybergenetics, objects to disclosure of software V&V materials, including source code, on the grounds that TrueAllele is a proprietary and copyrighted tool. First, that is not a valid basis to quash a subpoena and the government has failed to cite a case proving otherwise. Second, their objection is simply of no moment, as any intellectual property interests can be fully protected by an appropriate protective order. It is well established that trade secrets are not absolutely privileged from discovery in litigation. *Coca-Cola Bottling Co. of Shreveport, Inc. v. Coca-Cola Co.*, 107 F.R.D. 288, 292 (D. Del. 1985) (citing *Fed. Open Market Comm. v. Merrill*, 443 U.S. 340, 362 (1979); *Centurion Indus., Inc. v. Warren Steurer & Associates*, 665 F.2d 323, 325 (10th Cir. 1981); *Pennwalt Corp. v. Plough, Inc.*, 85 F.R.D. 257, 259 (D. Del. 1979). As the Supreme Court has recognized, "orders forbidding any disclosure of trade secrets or confidential commercial information are rare." *Coca-Cola Co.*, 107 F.R.D. at 293 (citing *Merrill*, 443 U.S. at 362 n. 24).

Court-ordered protective orders for expert materials that are claimed trade secrets are common in criminal cases. Courts readily exercise this discretion when necessary to ensure both that sensitive information is protected and that the defendant's right to present a full defense is preserved. *See*, *e.g.*, *Johnson*, No. 15-cr-565 (S.D.N.Y. June 7, 2016) (ordering government to produce PG system source code under protective order because of trade secret claims); *United*

States v. Diakhoumpa, No. 15-cr-629, 2016 WL 1105486, at *3 (S.D.N.Y. Mar. 15, 2016) (ordering government to produce under protective order trade secret information provided by trademark holders to government's experts in smuggling and counterfeiting case); *United States v. Durst*, No. 15-cr-91, 2015 WL 4879465, at *3–4 (E.D. La. Aug. 14, 2015) (denying motion to quash subpoena seeking proprietary trade secrets and issuing protective order to protect contents from public dissemination).

Even clearly commercial interests can be sufficiently protected by an appropriate order. *See United States v. Siegel*, No. 96-cr-411, 1997 WL 12804, at *4 (S.D.N.Y. Jan. 14, 1997) (in a criminal antitrust action, where disclosure of third-party competitor's bid formula would give defendant significant commercial advantage in the future, the court granted production only to counsel and an appropriate expert.)

In the context of civil litigation, courts regularly order the production of valuable trade secrets, specifically including source code, subject to orders that protect the disclosing party from commercial disadvantage. *See, e.g.*, *Dynamic Microprocessor Assoc. v. EKD Computer Sales*, 919 F. Supp. 101, 106 (E.D.N.Y. 2007) (ordering plaintiff to produce source code in copyright infringement litigation but limiting availability of source code to defense counsel and defendant's expert); *Quotron Sys., Inc. v. Automatic Data Processing Inc*, 141 F.R.D. 37, 41 (S.D.N.Y. 1992) (denying motion to quash subpoena seeking programming information involving "trade secrets between competitors" noting that "confidentiality concerns raised by these subpoenas can be dealt with by means of a protective order"); *see also Brown Bay Software v. Symantec Corp.*, 960 F.2d 1465 (9th Cir. 1992) (affirming scope of protective order fashioned by district court to protect trade secrets, including source code). Indeed, some of the world's most valuable trade secrets and intellectual property have been produced under appropriate protective orders. *See Coca-Cola*, 107

at 289, 300 (ordering disclosure of Coca-Cola's secret formula—"one of the best-kept trade secrets in the world"—under a protective order that "both allows access to information and prevents disclosure of trade secrets" and stating that "it may be advisable to limit the disclosure of the formulae to plaintiffs' trial counsel and independent experts").

As with Apple, Google, and Coca-Cola, any intellectual property interests Cybergenetics has in TrueAllele can be readily protected by an appropriate protective order. And though the government states that the source code "has never been disclosed," *see* ECF No. 47 at 3, it fails to mention that in the past year, Cybergenetics expressed a willingness to disclose the TrueAllele source code directly to the developer of its main competitor software, STRmix, in patent litigation in the Northern District of Ohio under a protective order. *See* Stipulated Patent Protective Order ¶¶ 7(c)–(d), *Cybergenetics v. Inst. of Envtl. Sci. & Research*, No. 5:19-cv-1197-SL (N.D. Ohio Dec. 23, 2019), ECF No. 33. If Cybergenetics was willing to share its source code in hopes of financial gain and protecting its asserted patent rights, there is no reason it should not disclose the source code when Mr. Ellis's constitutional rights to confront the evidence against him and to due process of law are on the line.

Because this case involves probabilistic genotyping software, the Defense urges this Court to follow *Johnson,* No. 15-cr-565, ECF No. 57 (S.D.N.Y. June 7, 2016) (Caproni, J.) (granting defendant's Rule 17(c) subpoena for probabilistic genotypic software Forensic Statistical Tool ("FST") source code). The *Johnson* case is both helpful and analogous to the issue of first impression facing this court regarding a Rule 17(c) subpoena to probabilistic genotyping software related to TrueAllele. In her Opinion ordering disclosure of the source code, Judge Valerie Caproni writes:

> FST is a relatively new tool that has not been extensively examined or tested in federal court, and the results obtained from the use of FST on DNA samples

> recovered from crime scenes are potentially devastating to a criminal defendant. The fact that the results obtained from use of the FST can be devastating to a criminal defendant increases the need of the Court to be diligent about FST's reliability prior to admitting FST results into evidence. Because the source code is relevant, specifically identified, admissible at least during a *Daubert* hearing, and not otherwise procurable by the exercise of due diligence, the defense is entitled to issue a subpoena pursuant to Fed. R. Crim. P. 17(c) to obtain the source code. The Court is prepared to enter a protective order if OCME wishes, although the Court questions why a public laboratory would need a protective order in this context.

See Johnson, No. 15-565, ECF. No. 57, Order Disclosing FST Source Code (internal citations, quotation marks, an alterations omitted), attached as Exhibit 5.

Additionally, even though Cybergenetics has not appeared in this case to advance its intellectual property interests, the Defense is willing to adhere to a protective order issued by this Court because it is mindful of Cybergenetics concerns, but not at the expense of Mr. Ellis's ability to test the reliability of their software. Again, given the similarities between this case and *Johnson*, the Defense proposes modeling the language of the protective order similar to the protective order issued in that case with one minor alteration.[7] *See* Protective Order Regarding the Confidentiality of the Forensic Statistical Tool Source Code and Related Documents, *United States v. Johnson,* No. 15-cr-565, (S.D.N.Y. July 18, 2016), attached as Exhibit 6.

This sort of exchange of source code under a protective order is quite common. *See, e.g*., Stipulated Protective Order Regarding Disclosure and Use of Discovery Materials, *Jongerius Panoramic Technologies, LLC v. Google, Inc*, No. 12-cv-3797, Feb. 13, 2013, ECF No. 137 (ordering stipulation between Google, Apple and Plaintiff to govern confidential information, including provisions governing source code). Indeed, some District Courts' model protective

[7] The Defense believes that the language in paragraph 10 of the *Johnson* protective order should be altered to say "This Protective Order shall survive the termination of the litigation. Within 30 days of the final disposition of this action, and any appeals thereof, all original Highly Confidential Material produced during the litigation shall be promptly returned to the producing party, or, upon permission of the producing party, destroyed. All copies of Highly Confidential Material shall be promptly returned to the producing party or destroyed."

orders include such provisions. *See* United States District Court for the Northern District of California, *Model Stipulated Protective Order for Litigation Involving Patents, Highly Sensitive Confidential Information and/or Trade Secrets*.[8] As the government pointed out, *see* ECF No. 108 at 20, our own District Court has rules related to source code disclosure. *See*, *e.g.*, Local Patent Rules, U.S. District Court for the Western District of Pennsylvania, Appendix LPR 2.2 (Model Protective Order) (designating "Source Code Information" as the most sensitive category of information, and providing strict rules for its inspection and handling).[9]

A standard protective order under supervision of the court should adequately protect the code from being revealed in public. *See also* Order, at 2, *United States v. Michaud*, No. 3:15-cr-05351, ECF No. 205 (W.D. Wash. May 18, 2016) (reiterating finding that a protective order was sufficient to protect secrecy of source code that had been ordered disclosed). Mr. Ellis is simply requesting a similar process be followed for the production of source code in this case.

In a last ditch effort, the government argues that Cybergenetics, the trade secret owner, should be given an opportunity to be heard, citing to 18 U.S.C. § 1835(b). *See* ECF. No. 108 at 20. However, Cybergenetics has already had six months to avail itself of that opportunity and has failed to do so.

Additionally, the citations to 18 USC 1835(b) and the congressional report are in apposite because they govern what the government can do in economic espionage and trade secret theft cases, which this is not.

II. THE SUBPOENA, WITH THE PROPOSED MODIFICATIONS, IS IN COMPLIANCE WITH RULE 17(C).

[8] http://www.cand.uscourts.gov/filelibrary/776/ND_Cal_Patent Highly_Sensitive_Model_Pro t Ord Revised.docx.
[9] https://www.pawd.uscourts.gov/sites/pawd/files/Local%20Patent%20R%20-%2012-5-2015.pdf.

In compliance with the Sixth Amendment and Rule 17(c) of the Federal Rules of Criminal Procedure, the Defense served a subpoena *duces tecum* to third-party software company Cybergenetics for software V&V materials on their flagship product, TrueAllele. The specific materials still at issue, materials the government has conceded the Defense sought first from the government, *see* ECF No. 108 at 21, are the materials listed in ¶ 23 of the Defendant's Response to Motion to Quash. *See* ECF No. 71 at 6–7, ¶ 23. Since its service, the Defense has agreed to several modifications to the subpoena. *See* ECF No. 71 at 8, n.4.[10] This Court has authority to modify the subpoena under Rule 17(c)(2). Albeit not mentioned in the modifications, or original subpoena, it was always the Defense's intent to procure the materials under a protective order. As previously mentioned, the Defense and their experts, are willing to adhere to and sign a protective order for the materials sought.

The Defense in their response to the government's motion to quash, *see* ECF No. 71, provided the Court with detailed case analysis of the two Supreme Court cases addressing Rule 17(c) (*Bowman Dairy Co*. & *Nixon*) and more than a handful cases interpreting those opinions specifically when a third-party is being subpoenaed. *See* ECF No. 71 at 13–19. For the sake of brevity, the Defense will not re-argue every single *Nixon* factor in this reply brief. The Defense has dedicated over fourteen pages of argument in support of why its now-modified subpoena to Cybergenetics is in compliance with Rule 17(c) and the four-factor test in *Nixon*. *See* ECF No. 71 at 19–32. As part of the Court's review of this particular brief, the Defense respectfully asks this

[10] For reference, the Defense agreed to this Court modifying the subpoena the following ways:

1. Exclude statements of witnesses or prospective witnesses.
2. Strike the two-week disclosure requirement, and give Cybergenetics four weeks to produce records requested.
3. Instead of producing the materials to the defense, the materials shall be produced to the Court, which has discretion to allow the parties to inspect the materials.
4. Modify the subpoena to only include items still outstanding which are listed in ¶ 23 of this response to the motion.

Court to review the Defense's response to the government's motion to quash [ECF No. 71] as it was filed on July 17, 2020.

The Defense does intend to reply to some of the government's claims however, and has hired three more experts since writing their response in July 2020. Based on this, the Defense will provide a brief summary of why the modified subpoena for the V&V materials, including source code, meets the *Nixon* factors with a focus on just replying to the government's claims, and adding new materials from three newly hired experts.

[1] <u>the V&V materials, including source code are evidentiary and relevant.</u>

A subpoena may be issued "for determination of an issue of fact raised by a pre-trial motion." Wright & Miller, 2 Fed. Prac. & Proc. Crim. § 272*;see also United States v. Cuthbertson*, 651 F.2d 189, 192 (3d Cir. 1981) (stating that it is not an abuse of discretion to order pretrial disclosure of materials under Rule 17(c)).

The V&V materials, including source code, are relevant because they are necessary to test the reliability of the software in order to determine whether the software makes appropriate assumptions and that it was developed in a way that makes it scientifically valid and reliable (or not). Specifically, as Defense Expert Nathan Adams pointed out in his Declaration, the requested materials are necessary to a determination of whether there are any software/technology issues based on the leading industry standards for probabilistic genotyping. *See* Mr. Adams's Declaration attached as Exhibit 2. The government wants to admit TrueAllele software findings. The Defense believes that this software ought to be subject to a *Daubert* analysis. Thus, the issue of fact for this Court to consider is whether the software's purported conclusion is admissible and whether or not it is constitutionally infirm. In order for the Court to make such a determination in the instant case, the Defense intends to offer the Court a comprehensive challenge to the reliability of TrueAllele.

The only meaningful way to do that is to have our experts (the Defense has hired four experts so far) evaluate the software. Because the software is "black box" or "closed source," the results are not reproducible—*i.e.*, they cannot be tested for accuracy and reliability. Accuracy and reliability are the lynchpins of the Defenses 702 and *Daubert* challenge.

The fact that other relevant material has been produced in discovery is of no import to this request. In fact, it is precisely from our intensive review of those materials that the Defense concluded that access to the V&V materials, including source code, would be necessary. The value of the validation studies, for example, is minimal without connecting those materials to the program itself. Moreover, the available operating procedures and user manuals only speak in general terms to how TrueAllele is supposed to work, but do not address the central question here: does the software reliably do what it purports to do?

The sough after materials are admissible under Fed. R. Evid. rules 102, 104, 401–402, 702, 803(1), 803(6), 803(7), and 807. They would also be admissible as non-hearsay, and as general impeachment evidence.

[2] the V&V materials, including source code are not otherwise procurable reasonably in advance of trial by exercise of due diligence.

The government confirmed that the Defense sought the requested documents from the government first prior to filing a subpoena for them. *See* ECF No. 108 at 21. Cybergenetics is also refusing to provide the materials.

[3] The Defense cannot properly prepare for trial without such production and inspection in advance of trial and that the failure to obtain such inspection may tend unreasonably to delay the trial.

The government wants this Court to believe that V&V materials, including source code, are not needed in order for the Defense to properly prepare for trial. The government writes, "[t]here is no genuine controversy as to the validity and reliability of the TrueAllele method" and

that the V&V materials, including source code, are just "nonsense" because TrueAllele is reliable. *See* ECF No. 108 at 4, 6. There is absolutely a genuine controversy over the validity and reliability of TrueAllele. *See R. v. Dechamp*, 2019 NSSC 367 (N.S.) (excluding TrueAllele). The PCAST Report from 2016 presented concerns about the scientific validity of probabilistic genotyping because it has not been subjected to the sorts of scientific testing that would be appropriate in their estimation. *See* PCAST Report, *supra*, at 75–83. The PCAST Report mentions TrueAllele by name as one of the PG systems that courts should be weary of. TrueAllele is a black box algorithm PG system. That alone makes it controversial. *See United States v. Gissantaner*, 417 F. Supp. 3d 857 (W.D. Mich. 2019) (excluding probabilistic genotyping software STRmix as not sufficiently reliable under *Daubert* in a three-person complex mixture case); *People v. Collins*, 15 N.Y.S.3d 564 (N.Y. Sup. Ct. 2015) (excluding PG software as not generally accepted as reliable in the forensic scientific community under the *Frye* standard in a three-person complex mixture case); *see also* Katherine Kwong, *The Algorithm Says You Did It: The Use of Black Box Algorithms to Analyze Complex DNA Evidence*, 31 Harv. J. L. & Tech. 275, 295 (2017) ("The lack of independent studies establishing scientific validity for many uses of algorithmic DNA interpretation technologies and the lack of transparency about the subjective decisions embodied in these programs' codes exacerbate the issues caused by each. Without transparency, it is more difficult to rigorously evaluate scientific validity; without rigorous studies, it is more difficult to challenge specific issues caused by a lack of transparency. Because of the potential impacts these issues may have on defendants' outcomes, these issues should be resolved.").

Furthermore, the secrecy behind TrueAllele and other PG systems that do not allow meaningful review of their product is worrisome. As the Electronic Privacy Information Center has argued to Congress when advocating for greater transparency, "[s]ecrecy of the algorithms

used to determine guilt or innocence undermines faith in the criminal justice system." Letter from Marc Rotenberg & Caitriona Fitzgerald, President and Policy Dir., Elec. Privacy Info. Ctr., to Hon. Trey Gowdy, Chair, House Comm. on the Judiciary, Subcomm. on Crime, Terrorism, Homeland Sec., & Investigations 3.[11]

As far as the request for the source code being "nonsense," the Defense has presented the court with numerous articles and scholarship about the need for source code. More specifically however, the Defense has presented to this Court, four experts across three declarations that have emphasized the need for the V&V materials.

Regarding the need for source code Dr. Krane, declares:

> Access to TrueAllele®'s source code would be similarly helpful in assessing whether its algorithmic design and the implementation of its algorithms as a software program are appropriate for use in a criminal trial. Publicly available materials that describe the TrueAllele® software development process are not sufficient for establishing that TrueAllele® has been developed in accordance with software engineering best practices or that it has been (or even could be) verified and validated in a way that is consistent with software engineering standards. Access to materials supporting the TrueAllele® software development and V&V processes would allow an objective evaluation as to whether public claims of the reliable operation of TrueAllele® are supported by non-public materials. . . . While it is important to consider the perspectives of experts in the areas of molecular biology, population genetics, statistics, forensic science, computer science, and software engineering it is particularly important that software engineers have the opportunity to evaluate the implementation and testing of probabilistic genotyping systems like TrueAllele®.

See Exhibit 3 at ¶ 19.

Regarding the need for source code Drs. Heimdahl and Matthews declare:

> Review of TrueAllele's source code is necessary to identify the existence and import of any flaws in the program. Review of the software must be meaningful, and cannot consist of merely reviewing the public materials Cybergenetics provided to the Defense. Without actually reviewing the verification and validation "V&V" materials, requested by Nathan Adams in his declaration, Mr. Ellis' review of the materials publicly disclosed would render expert review essentially

[11] https://perma.cc/4L5J-EFLR.

> meaningless. That is, TrueAllele's code cannot be meaningfully reviewed without full access to the executable source code and software development documentation.

See Exhibit 4 at ¶ 52.

> In order to evaluate the reliability of TrueAllele, the Defense's expert would need access to TrueAllele's software development documentation, including testing, software design, bug reporting, change logs, and program requirements. Such documentation not only acts as a "road map" for the expert to understand the source code, but also allows the expert to determine whether Cybergenetics followed industry standards in developing TrueAllele. Because software is error prone, there are industry standards for software verification and validation. Access to TrueAllele's software development documentation would allow an expert to determine whether those standards were followed.

See Exhibit 4 at ¶¶ 56–57.

> Mr. Ellis' very freedom hinges upon the results yielded by a black-box software program. Mr. Ellis and this Honorable Court deserve to understand how that software actually works, and the only means of doing so is by providing full access to the executable source code and the validation and verification materials. We disagree with the government's statement in the motion to quash subpoena that "[t]here is no genuine controversy as to the validity and reliability of the TrueAllele method." see Doc. No. 108 at 4. No one outside of Cybergenetics has examined the source code or validation and verification materials for TrueAllele. None of the over 35 studies provided looked at the source code or any of the TrueAllele validation and verification artifacts and are therefore unable to comment on how the general computational method is implemented in software. This is a crucial step in which many errors can be made and in which many errors have been made in similar software projects. Given its nature, TrueAllele is particularly likely to contain undetected flaws: users are unlikely to notice failures, the incentive structure makes reporting flaws less likely, and the TrueAllele software has not been subject to thorough, independent review.

See Exhibit 4 at ¶ 60.

Rigorous independent testing is not merely a best practice for software like TrueAllele. The world's leading computer science review community—the Institute of Electrical and Electronics Engineers ("IEEE")—*requires* technically, managerially, and financially independent testing for any software where "catastrophic consequences" could result even occasionally. IEEE Standards Ass'n, *IEEE Std. 1012-2016: IEEE Standard for System, Software, and Hardware*

Verification and Validation 196, 199 (2016); *see also* Nathaniel Adams, *What Does Software Engineering Have to Do with DNA?*, The Champion (May 2018) (discussing importance of subjecting PG systems to software engineering best practices and independent reviews). The IEEE defines "catastrophic consequences" as "[l]oss of human life, complete mission failure, loss of system security and safety, or extensive financial or social loss." *Id.* at 196. For such software, the IEEE requires that the developer be fully independent from the organization responsible for verifying and validating that the software operates as expected. *Id.* at 199.

In her opinion in *Dechamp* excluding TrueAllele, Justice Campbell wrote among other things,

> [TrueAllele] is not subject to either accreditation or auditing with respect to the development or maintenance of that software. The source code that operationalizes the mathematics and DNA science, has been seen in its entirety only by Dr. Perlin. That source code and the program that the source code runs are not subject to any kind of regulation, auditing or accreditation.

See, Exhibit 1 at ¶ 43.

Justice Campbell continued,

> When a computer program or instrument is intended for use in the forensic context, its reliability should be established through a rigorous process of third-party accreditation. The reservations about the use of DNA analysis from a company that is not subject to standards for accreditation, using software that is not subject to standards that are enforced by any independent body other than the academic community at large are not unreasonable. They justify questions being raised.

See, Exhibit 1 at ¶ 22.

When, as here, hidden software code produces the prosecution's key forensic evidence of guilt, the defendant's fate can be determined by a black box that the Defense has no opportunity to examine or challenge. Software errors are common and forensic software has no special immunity from the bugs and mistakes that plague software in other fields. As the government conceded, a Virginia court recently ordered TrueAllele's source code disclosed, and because the

government there did not file a motion to quash, Cybergenetics was "forced to hire its own counsel at its own expense" to file a motion for reconsideration. *See* ECF No. 108 at 6 n.2. What incentive does Dr. Perlin have to try and prevent a Defendant from independently evaluating his software for the court to consider? What is he afraid of? As discussed above, trade secrets are routinely disclosed between competitors. The fear of having his source code replicated by the Defense team expert in a criminal prosecution is unreasonable. It is especially unreasonable due to the fact that he was willing to provide his source code, under a stipulated protective order, to his biggest competitor in the patent infringement lawsuit he filed against them. *See* Stipulated Patent Protective Order ¶¶ 7(c)–(d), *Cybergenetics v. Inst. of Envtl. Sci. & Research*, No. 5:19-cv-1197-SL (N.D. Ohio Dec. 23, 2019), ECF No. 33, attached as Exhibit 7.

Because the sought-after documents are material to the preparation of Mr. Ellis's defense, the Defense must be allowed to review the V&V materials, including source code, in order to understand and meaningfully confront the prosecution's forensic evidence.

[4] <u>The application is made in good faith and is not intended as a general "fishing expedition.</u>"

"The test for enforcement is whether the subpoena constitutes a good faith effort to obtain identified evidence rather than a general 'fishing expedition' that attempts to use the rule as a discovery device." *Cuthbertson*, 630 F.2d at 144. "A subpoena that fails to describe any specific documents is too broad, but it is not necessary that the subpoena designate each particular paper desired. It is sufficient if kinds of documents are designated with reasonable particularity." Wright & Miller, 2 Fed. Prac. & Proc. Crim. § 275.

Here, the request for materials is made in good faith and is specifically tailored using precise terms of art. As Defense Expert Nathan Adams declared, the materials sought are specifically tailored using precise terms of art based on industry standards for evaluation and

verification and validation of probabilistic genotyping software systems like TrueAllele. *See* Exhibit 2 ¶¶ 22–24, 41. As much as the government wants to argue it, the materials requested are not a "fishing expedition." The government has already conceded that TrueAllele works based on source code, *see* ECF No. 47 at 12, thus, the Defense is not merely hoping that it exists—we know it exists. *See Cuthbertson*, 630 F.2d at 146 ("We do not think that this 'mere hope' justifies enforcement of a subpoena under rule 17(c)."). Thus, the Defense is not "fishing" for something that may exist or may not exist, we know it exists and we know who is in possession of it—Cybergenetics.

III. THE CONSTITUTION, AND RULES OF CRIMINAL PROCEDURE AND EVIDENCE, SUPPORT GOVERNMENT DISCLOSURE OF THE MATERIALS REQUESTED IN DEFENSE'S MOTION TO COMPEL DISCOVERY.

Though Mr. Ellis believes the materials sought are most appropriately obtained under Rule 17 from Cybergenetics, the government has insisted that Mr. Ellis must seek the relevant materials under Rule 16. *See* ECF No. 47 at 3 ("[T]he subpoena demands information from the government's expert, but the required expert disclosures are governed by Rule 16(a)(1)(G), and Rule 17(c)(1) does not expand those requirements."). But, the government now concedes that the information Mr. Ellis is seeking is not within the government's "possession, custody, or control" as required by Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure. *See* ECF No. 108 at 8–9. That is why Mr. Ellis originally sought the material directly from Cybergenetics; Mr. Ellis's Rule 16 request was filed based on the government's insistence that Rule 16 was the appropriate vehicle to obtain the source code and requested documentation.

Mr. Ellis does not concede that he is not entitled to the requested materials under Rule 16, or other Constitutional principles. However, as stated, he is either entitled to them pursuant Rule 16 or Rule 17. In so far those arguments are concerned, the Defense respectfully points the Court to Defense Motion to Compel Software Verification Materials at ECF No. 83.

IV. REPLYING THE GOVERNMENT'S ARGUMENTS REGARDING MR. ELLIS' MOTION TO COMPEL.

The government claims that this is an "open file" case and claims that they are willing to allow the Defense to review their files. *See* ECF No. 108 at 28. On April 10, 2020, the Defense emailed the prosecution asking for specific discovery materials. The government claims that some items requested are not discoverable, yet says this is an "open file" case. How can something be "open file" yet not discoverable? It's either a closed file case, were the defense is entitled to only Rule 16, or it's an open file case, were the prosecution shares their entire case file.

Pursuant to Rule 16, Mr. Ellis asked to inspect a sweatshirt that was found in a parking garage, photographed, collected for evidence, and according to the police officers worn by the individual who drove the car in which the gun was found.

Photo of gray sweatshirt at issue

The government writes that the sweatshirt is "not available." *See* ECF No. 108 at 28. How can it not be available? The sweatshirt was photographed, and logged into evidence. Mr. Ellis requests an order compelling the sweatshirt, or an order for the government to explain to the Defense why it is "not available."

Pursuant Rule 16, Mr. Ellis requested records related to the drug dog. The government writes that this material is "not discoverable under any legal theory." *See* ECF No. 108 at 29. The government is wrong. The government has long been on notice that a defendant is entitled to canine training records and that their disclosure is mandatory. *See United States v. Cedano–Arellano*, 332

F.3d 568, 573 (9th Cir.2003) (requiring disclosure of dog training and certification records pursuant to Fed.R.Crim.P. 16); *United States v. Owens*, 167 F.3d 739, 749 (1st Cir.1999) (noting that expert reviewed canine's records); *United States v. Gonzalez–Acosta*, 989 F.2d 384, 388 (10th Cir.1993) (observing that district court required government to produce canine log); *United States v. Lambert*, 351 F.Supp.2d 1154, 1162 (D.Kan.2004) (allowing discovery of canine training and certification records for the year prior to the search); *United States v. McGlothen*, No. 8:08CR183, 2008 WL 4533971, at *3–*4 (D.Neb. Oct.3, 2008) (granting defendant's discovery request for training forms, drug detector dog grade sheets, and deployment forms, among other canine-related records); *United States v. Campos*, 237 Fed.Appx. 949, 954, 2007 WL 2083661 (5th Cir.2007) (noting that district court reviewed testimony and evidence, including evidence of canine's false alerts); *see also United States v. Cortez–Rocha*, 394 F.3d 1115, 1118 n. 1 (9th Cir.2005). These types of records are "crucial to [a defendant's] ability to assess the dog's reliability, a very important issue in his defense, and to conduct an effective cross-examination of the dog's handler." *Cedano–Arellano*, 332 F.3d at 571.

Lastly, pursuant Rule 16, the Defense requested disclosure of forensic laboratory related discovery in reference to Lab No. 18LAB06905 from the County of Allegheny Office of the Medical Examiner regarding the DNA tests performed in this case. *See* ECF No. 98 at 3-4. In response to this request, the government wrote, "[a]s the defendant concedes, the government already provided the report related to this examination." *See* ECF No. 108 at 29. This is again inaccurate. The government provided the final report, but did not provide the specific materials requested by the Defense. *See* ECF No. 98 at 3-4. The materials were requested by demand from the Defense experts who routinely request such materials in their review of forensic DNA or serological testing. According to the Defense expert, such materials and are commonly requested

by other independent experts doing similar work. The documents are material to defense because any errors found within the analyzation and process' of the handling of the DNA at the County of Allegheny Office of the Medical Examiner may contribute to additional claims to exclude DNA software results of TrueAllele. For example, data, notes, and records of testing samples and controls associated with this case are necessary in order to determine what was actually "done" in this case. These materials form the foundation of any conclusions specific to this case. Laboratory validation and procedures: Standard Operating Procedures (also called protocols, manuals, *etc*.) form the rule set for analysts to follow when conducting examinations, testing, analysis, reporting, *etc*. Validation records describe the limitations of reliability of the laboratory's procedures, as determined by the lab on their own equipment. Validation records therefore inform the laboratory procedures/protocols. These materials describe what a laboratory can hypothetically do and how its analysts should perform their work. Materials including external audit records and records of "unexpected results" or "corrective actions" that do not pertain directly to this case help characterize the lab's general ability to undertake its work. Any deficiencies or deviations from standards noted in an audit, could be considered relevant to a lab's general operations. Any trends apparent in "unexpected results" or "corrective actions" logs that are not noted in case-specific records, might characterize a lab's, or a specific analyst's, general ability to adhere to policy and procedure, which should inform the confidence with which we accept their conclusions. If these materials do not exist, or do exit, but are not provided for review, we should not place more confidence in the laboratory's abilities, but rather recognize that we are unable to appropriately characterize the degree of confidence that should be placed in their abilities.

Early disclosure of these materials is necessary for review and evaluation of the DNA work performed by the County of Allegheny Office of the Medical Examiner because they are the

laboratory that sent the gun DNA to Cybergenetics. Any flaws with the work done at the original lab, directly impact TrueAllele results. Because the Defense expert requires these materials to opine on the reliability of the results produced by TrueAllele in this case, the materials are discoverable under Rule 16(a)(1)(E)-(F)-(G). *See United States v. Liquid Sugars, Inc.*, 158 F.R.D. 466, 471 (E.D. Ca. 1994) ("if the government plans to use the results of scientific tests as evidence, data and reports which directly underlie those results are generally important to an understanding of the evidence."); *United States v. W.R. Grace*, 233 F.R.D. 586, 587– 88 (D. Mont. 2005) (compelling production of "documents underlying asbestos sampling tests performed by the government or its experts on the soil and air in the Libby area" because they were material to preparing the defense.); *United States v. Siegfried*, 2000 WL 988164 (N.D. III. 2000) ("it appears that the government's case will be based in significant part on the results of the tests. That being the case, considerations of fundamental fairness require that the defense have access to material concerning the manner and means of testing so that it can make an independent determination of the tests' reliability and have a fair opportunity to challenge the government's evidence. The testing protocols may not be, strictly speaking, "results or reports" of testing and thus may well not be covered by Rule 16(a)(1)(D). Even if not, however, the Court believes for the reasons stated that the protocols are "material to the preparation of the defense" and are thus within the scope of Rule 16(a)(1)(C) even if they are outside the scope of Rule 16(a)(1)(D).").

CONCLUSION

For all the reasons articulated in the Defense's briefs, Mr. Ellis respectfully requests the Court to deny the motion to quash, enter a protective order, and compel Cybergenetics to produce the requested materials.

Respectfully Submitted,

/s/ *Khasha Attaran*

Khasha Attaran
Assistant Federal Public Defender